UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
BOSTON DIVISION

CASEY WHALEN and LUKE MILLSPAUGH, Individually, and on Behalf of All Others Similarly Situated,	)	
Plaintiffs,	)	Case No.
v.	)	**JURY TRIAL DEMANDED**
EMMANUEL COLLEGE,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiffs Casey Whalen and Luke Millspaugh ("Plaintiffs"), through their undersigned counsel, bring this action against Emmanuel College ("Emmanuel" or "Defendant") pursuant to the investigation of their attorneys, personal knowledge as to themselves and their own acts and otherwise upon information and belief, and allege as follows:

INTRODUCTION

1. Emmanuel College is a private not-for-profit college affiliated with the Roman Catholic Church in Boston, Massachusetts.

2. On or about January 31, 2024, Emmanuel announced publicly that on or about April 27, 2023, it had been the recipient of a hack and exfiltration of sensitive personal information ("SPI") involving approximately eighty-nine thousand individuals who were its students, former students, or applicants. (the "Data Breach").

3. Emmanuel reported that this SPI included at least name, date of birth, GPA, student ID, financial aid awards, and full Social Security Number.

4. Plaintiffs and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

5. The information stolen in cyber-attacks allows the modern thief to assume victims' identities when carrying out criminal acts such as:

- Filing fraudulent tax returns;
- Using your credit history;
- Making financial transactions on behalf of victims, including opening credit accounts in victims' names;
- Impersonating victims via mail and/or email;
- Impersonating victims in cyber forums and social networks;
- Stealing benefits that belong to victims; and
- Committing illegal acts which, in turn, incriminate victims.

6. Plaintiffs' and Class members' SPI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the SPI of Plaintiff and Class members.

7. As of this writing, there exist many class members who have no idea their SPI has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

8. Plaintiffs bring this action on behalf of all persons whose SPI was compromised as a result of Defendant's failure to: (i) adequately protect consumers' SPI, (ii) adequately warn its current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendant's conduct amounts to negligence and violates state statutes.

9. Plaintiffs and similarly situated individuals have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished inherent value of SPI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (iii) lost opportunity costs associated with attempting

to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under state consumer protection and data breach notification acts; and (v) the continued and certainly an increased risk to their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

11. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is located within this District.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

PARTIES

13. Plaintiff Casey Whalen is a natural person residing in Rockingham County, New Hampshire. On or about January 31, 2024, Plaintiff was informed via letter that he had been a victim of the Data Breach.

14. Plaintiff Luke Millspaugh is a natural person residing in Suffolk County, Massachusetts. On or about January 31, 2024, Plaintiff was informed via letter that he had been a victim of the Data Breach.

15. Defendant Emmanuel College is a not-for-profit private college with its principal place of business at 400 The Fenway, Boston, Massachusetts.

FACTUAL ALLEGATIONS

16. Defendant is a private not-for-profit college affiliated with the Roman Catholic Church in Boston, Massachusetts.

17. When prospective students apply to Defendant, they provide Defendant with SPI such as:

a. Contact and account information, such as name, address, telephone number, email address, and household members;

b. Authentication and security information such as government identification, Social Security number, security codes, and signature;

c. Demographic information, such as age, gender, and date of birth; and

d. Payment information and income information, such as credit card, debit card, bank account numbers, and income information, possibly including tax returns.

18. On or about January 31, 2024, Emmanuel announced publicly that on or around April 27, 2023, "Emmanuel College experienced a security incident that involved your personal information."[1]

19. Emmanuel became aware of the Data Breach no later than January 16, 2024, and it notified students, former students, and applicants within two weeks. However, it says that it did not *discover* the breach for nearly eight months after it happened.

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/63bfe061-8381-4397-b07b-2a78d22f5785.shtml, last accessed February 25, 2024.

20. As a result, Plaintiffs' and class members' SPI was in the hands of hackers for nearly eight months before Defendants began notifying them of the Data Breach.

21. Defendant has been distressingly vague on its response to the Data Breach, stating only that "As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents.."[2]

22. As of this writing, Defendants have offered no concrete information on the steps they have taken or specific efforts made to reasonably ensure that such a breach cannot or will not occur again.

23. Defendants are offering minimal additional assistance to Plaintiffs and class members beyond an inadequate 12 months of credit monitoring.

24. This response is entirely inadequate to Plaintiffs and class members who now potentially face several years of heightened risk from the theft of their SPI and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

25. Emmanuel's Privacy Policy states:

> The College will use your personal information only for business-related purposes, including but not limited to conducting our usual operations and administering educational and other services, managing user accounts, contacting users to respond to requests or inquiries, processing and completing academic, financial and other transactions, providing you with newsletters, invitations or other announcements, conducting research or surveys, meeting legal obligations, and conducting marketing, promotional, fundraising, and advertising activities.[3]

---

[2] *Id.*

[3] https://www.emmanuel.edu/copyright-and-privacy-policy, last accessed February 25, 2024.

26. The Privacy Policy further notes that "All student records are protected under the Federal Family Education Rights and Privacy Act (FERPA), and consequently, cannot be released to a third party without the student's consent."[4]

27. Needless to say, the release of Plaintiffs' and Class members' SPI was done without their consent and in ways not consistent with Defendant's Privacy Policy.

28. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class members, to keep their SPI confidential and to protect it from unauthorized access and disclosure.

29. Plaintiffs and Class members provided their SPI to Defendants with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

30. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the medical services industry preceding the date of the breach.

31. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

32. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to

[4] *Id.*

resolve.[5] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[6]

33. The SPI of Plaintiff and members of the Class was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the SPI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

34. Defendant knew, or reasonably should have known, of the importance of safeguarding the SPI of Plaintiff and members of the Class, including Social Security numbers, dates of birth, and other sensitive information, as well as of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and members of the Class a result of a breach.

35. Plaintiffs and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their SPI.

36. The injuries to Plaintiffs and members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the SPI of Plaintiffs and members of the Class.

37. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

---

[5] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf, last accessed February25, 2024.

[6] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

38. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

39. The FTC further recommends that companies not maintain SPI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

40. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

41. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer SPI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

42. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

43. Best cybersecurity practices include installing appropriate malware detection

software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

44. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

45. The SPI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[7]

46. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity

[7] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs, last accessed February 25, 2024.

can cause a lot of problems.[8]

47. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

48. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[9]

49. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[10]

50. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential SPI to mimic the identity of the

---

[8] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed February 25, 2024.

[9] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft, last accessed February 25, 2024.

[10] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed February 25, 2024.

user. The personal data of Plaintiff and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and members of the Class represents essentially one-stop shopping for identity thieves.

51. The FTC has released its updated publication on protecting SPI for businesses, which includes instructions on protecting SPI, properly disposing of SPI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

52. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

53. Companies recognize that SPI is a valuable asset. Indeed, SPI is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other SPI on a number of Internet websites. The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

54. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

55. As noted above, the disclosure of Social Security numbers in particular poses a

---

[11] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29, last accessed February 25, 2024.

significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

56. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number, name, and date of birth.

57. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[12]

58. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

FACTS SPECIFIC TO PLAINTIFFS

59. On or about January 31, 2024, Plaintiff Casey Whalen was notified via letter from

[12] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html, last accessed February 25, 2024.

Defendant that he had been the victim of the Data Breach.

60. Plaintiff applied to Emmanuel in 2015, but chose not to attend.

61. There can be no legitimate business reason for Defendant continuing to maintain Plaintiff's SPI, including his Social Security number, for years past his application.

62. Had Plaintiff known that his SPI would not have been adequately protected by Defendant, he would not have applied to Emmanuel or he would have insisted that they not be stored in Defendant's system.

63. Since the time of the Data Breach, some individual or individuals have repeatedly, and for dozens of times, attempted to log in to Plaintiff's Paypal account. These efforts are only unsuccessful because he has enabled two-factor authentication. Nonetheless, these constant attempts have taken time and effort to address on Plaintiff's part.

64. On information and belief, these attempted intrusions have been possible due in part to the types of information stolen from Defendant's systems.

65. Additionally, Plaintiff is aware of no other source from which the theft of his SPI could have come. He regularly takes steps to safeguard his own SPI in her own control.

66. On or about January 31, 2024, Plaintiff Luke Millspaugh was notified via letter from Defendant that he had been the victim of the Data Breach.

67. Plaintiff applied to Emmanuel in 2016, but chose not to attend.

68. There can be no legitimate business reason for Defendant continuing to maintain Plaintiff's SPI, including his Social Security number, for years past his application.

69. Had Plaintiff known that his SPI would not have been adequately protected by Defendant, he would not have applied to Emmanuel or he would have insisted that they not be stored in Defendant's system.

70. Since the time of the Data Breach, some individual or individuals have repeatedly, and for dozens of times, attempted to log in to Plaintiff's Venmo account. These efforts are only unsuccessful because he has enabled two-factor authentication. Nonetheless, these constant attempts have taken time and effort to address on Plaintiff's part.

71. On information and belief, these attempted intrusions have been possible due in part to the types of information stolen from Defendant's systems.

72. Additionally, Plaintiff is aware of no other source from which the theft of his SPI could have come. He regularly takes steps to safeguard his own SPI in her own control.

CLASS ACTION ALLEGATIONS

73. Plaintiffs bring this class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes:

> All natural persons residing in the United States whose SPI was compromised in the Data Breach announced by Defendants on or about January 31, 2024.

74. Additionally, Plaintiff Casey Whalen brings this class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, on behalf of all members of the following subclass:

> All natural persons residing in New Hampshire whose SPI was compromised in the Data Breach announced by Defendants on or about January 31, 2024 (the "New Hampshire Subclass").

75. Additionally, Plaintiffs bring this class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, on behalf of all members of the following subclass:

> All natural persons residing in United States who provided their SPI to, but did not attend Emmanuel College, whose SPI was compromised in the Data Breach announced by Defendants on or about January 31, 2024 (the "Applicant Subclass").

76. The Class, the New Hampshire Subclass, and the Applicant Subclass may be referred to collectively as the "Class" or the "Classes."

77. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

78. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

79. **Numerosity**: The Class is so numerous that joinder of all members is impracticable. Defendants have, as of this writing, indicated to the Maine Attorney General that the number of affected class members is approximately 89,064.[13] The Classes are readily identifiable within Defendants' records.

80. **Commonality**: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual members of the Class. These include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their SPI;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the SPI of Plaintiffs and members of the Class;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of SPI belonging to Plaintiffs and members of the Class;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the SPI of Plaintiffs and members of the Class secure and to prevent loss or

[13] https://apps.web.maine.gov/online/aeviewer/ME/40/63bfe061-8381-4397-b07b-2a78d22f5785.shtml, last accessed February 25, 2024.

misuse of that SPI;

g. Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiffs' and members of the Classes' damages;

i. Whether Defendant violated the law by failing to promptly notify Plaintiffs and members of the Classes that their SPI had been compromised; and

j. Whether Plaintiffs and the other members of the Class are entitled to credit monitoring and other monetary relief.

81. **Typicality**: Plaintiffs' claims are typical of those of the other members of the Class because all had their SPI compromised as a result of the Data Breach due to Defendant's misfeasance.

82. **Adequacy**: Plaintiff swill fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' counsel are competent and experienced in litigating privacy-related class actions.

83. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual member of the Class are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

84. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as the California Subclass as a whole.

85. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification

because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and members of the Class to exercise due care in collecting, storing, using, and safeguarding their SPI;

b. Whether Defendant breached a legal duty to Plaintiffs and the members of the Class to exercise due care in collecting, storing, using, and safeguarding their SPI;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Class are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF
Negligence
(By Plaintiffs Individually and on Behalf of the Classes)

86. Plaintiffs hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 85.

87. Defendant routinely handles SPI that is required of its applicants, students, and former students such as Plaintiffs.

88. By collecting and storing the SPI of its applicants, students, and former students, Defendant owed a duty of care to the individuals whose SPI it collected to use reasonable means to secure and safeguard that SPI.

89. As an educational institution, Defendant is aware of that duty of care to the SPI of its customers.

90. Additionally, as covered entities, Defendant has a duty under FERPA privacy laws to protect the confidentiality of student information, including the kind stolen as part of the Data Breach.

91. Defendant has full knowledge of the sensitivity of the SPI and the types of harm that Plaintiffs and Class Members could and would suffer if the SPI were wrongfully disclosed.

92. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their applicants', students', and former students' SPI, and that of their beneficiaries and dependents, involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

93. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs' and Class Members' information in Defendant's possession was adequately secured and protected.

94. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' SPI.

95. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

96. Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of should have known of the inherent risks in collecting and storing the SPI of Plaintiffs and the Class, the critical importance of providing adequate security of that SPI, and the necessity for encrypting SPI stored on

Defendant's systems.

97. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' SPI, including basic encryption techniques freely available to Defendant.

98. Plaintiffs and the Class Members had no ability to protect their SPI that was in, and presumably remains in, Defendant's possession.

99. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

100. Defendant had and continues to have a duty to adequately disclose that the SPI of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their SPI by third parties.

101. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the SPI of Plaintiffs and Class Members.

102. Defendant has admitted that the SPI of Plaintiffs and Class Members was purposely exfiltrated and disclosed to unauthorized third persons as a result of the Data Breach.

103. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the SPI of Plaintiffs and Class Members during the time the SPI was within Defendant's possession or control.

104. Defendant improperly and inadequately safeguarded the SPI of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

105. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former employees' SPI in the face of increased risk of theft.

106. Defendant, through their actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former employees' SPI.

107. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

108. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the SPI of Plaintiffs and Class Members would not have been compromised.

109. There is a close causal connection between Defendant's failure to implement security measures to protect the SPI of Plaintiffs and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' SPI was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such SPI by adopting, implementing, and maintaining appropriate security measures.

110. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their SPI is used; (iii) the compromise, publication, and/or theft of their SPI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (v) lost opportunity

costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their SPI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI of its employees and former employees in its possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the SPI compromised as a result of the Data Breach for the remainder of Plaintiffs' and Class Members' lives.

111. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI in its continued possession.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(By Plaintiffs Individually and on Behalf of the Classes)

112. Plaintiffs hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 85.

113. When Plaintiffs and Class Members provided their SPI to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant under which—and by mutual assent of the parties—Defendant agreed to take reasonable steps to protect their SPI.

114. Defendant solicited and invited Plaintiffs and Class Members to provide their SPI

as part of Defendant's regular business practices and as essential to the services transactions entered into between Defendant on the one hand and Plaintiffs and Class Members on the other. This conduct thus created implied contracts between Plaintiffs and Class Members on the one hand, and Defendant on the other hand. Plaintiffs and Class Members accepted Defendant's offers by providing their SPI to Defendant in connection with their purchases from Defendant.

115. When entering into these implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

116. Defendant's implied promise to safeguard Plaintiffs' and Class Members' SPI is evidenced by a duty to protect and safeguard SPI that Defendant required Plaintiffs and Class Members to provide as a condition of entering into transactions with Defendant.

117. Plaintiffs and Class Members paid money to Defendant in order for Defendant to consider them for admission to Emmanuel College. Plaintiffs and Class Members reasonably believed and expected that Defendant would use part of funds received as a result of the purchases to obtain adequate data security. Defendant failed to do so.

118. Plaintiffs and Class Members, on the one hand, and Defendant, on the other hand, mutually intended—as inferred from applicants' and students' use of Defendants' services—that Defendant would adequately safeguard SPI. Defendant failed to honor the parties' understanding of these contracts, causing injury to Plaintiffs and Class Members.

119. Plaintiffs and Class Members value data security and would not have provided their SPI to Defendant in the absence of Defendant's implied promise to keep the SPI reasonably secure.

120. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

121. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

122. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs and Class Members sustained damages as alleged herein.

123. Plaintiffs and Class Members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

124. Plaintiffs and Class Members also are entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, remove the SPI of the Applicant Subclass from its systems, and provide credit monitoring and identity theft insurance to Plaintiffs and Nationwide Class members.

THIRD CLAIM FOR RELIEF
Unjust Enrichment, in the Alternative
(By Plaintiffs Individually and on Behalf of the Nationwide Classes)

125. Plaintiffs hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 85.

126. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of storing their SPI with Defendant in such a way that saved expense and labor for Defendant.

127. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Defendant also benefited from the receipt of Plaintiffs' and Class Members' SPI, as this was used by Defendant to facilitate its core functions.

128. The benefits given by Plaintiffs and Class Members to Defendant were to be used by Defendant, in part, to pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures.

129. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount to be determined at trial.

130. Under principles of equity and good conscience, Defendant should not be permitted to retain a benefit belonging to Plaintiffs and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that

Plaintiffs and Class Members granted to Defendant or were otherwise mandated by federal, state, and local laws and industry standards.

131. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds or benefits it received as a result of the conduct alleged herein.

FOURTH CLAIM FOR RELIEF
Violation of New Hampshire Consumer Protection Act, RSA § 358-A *et seq*.
(By Plaintiff Casey Whalen Individually and on Behalf of the New Hampshire Subclass)

132. Plaintiff Casey Whalen hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 85.

133. Plaintiff and the New Hampshire Subclass are residents of New Hampshire.

134. Defendant conduct business in New Hampshire by soliciting applications for acceptance within the State of New Hampshire and maintain computerized data that contain the personal identifying information of New Hampshirites.

135. The NHCPA prohibits a person or entity from using "any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within this state." N.H. Rev. Stat. Ann. § 358-A:2.

136. The New Hampshire statutory scheme provides a non-exhaustive list of acts that constitute violations of the statute, which includes but is not limited to the following:

> a. "Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that such person does not have[.]" N.H. Rev. Stat. Ann. § 358-A:2(V).
>
> b. "Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another[.]" N.H. Rev. Stat. Ann. § 358-A:2(VII).

c. "Advertising goods or services with intent not to sell them as advertised[.]" N.H. Rev. Stat. Ann. § 358-A:2(IX).

137. Defendant engaged in the conduct alleged in this complaint through transactions in and involving trade and commerce within the State of New Hampshire. N.H. Rev. Stat. Ann. § 358-A:2.

138. While involved in trade or commerce, Defendant violated the NHCPA by engaging in unfair, deceptive, and unconscionable business practices including, among other things, by:

139. Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the Private Information of Defendant's patients from unauthorized access and disclosure; and

140. Failing to disclose the material fact that its computer systems and data security practices were inadequate to safeguard and protect the Private Information of Plaintiffs and the New Hampshire Subclass from being compromised, stolen, lost, or misused.

141. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs and the New Hampshire Subclass' SPI entrusted to it, and that risk of a data breach or theft was highly likely.

142. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

143. Defendant's failures constitute an unfair practice and false, deceptive, and misleading representations regarding the security of Defendant's network and aggregation of SPI.

144. These unfair practices and misleading representations upon which Plaintiff and the New Hampshire Subclass relied were material facts (e.g., as to Defendant's adequate protection of SPI), and applicants and students relied on those representations to their detriment.

145. In committing the acts alleged herein, Defendant engaged in fraudulent, deceptive, and unfair practices by omitting, failing to disclose, or inadequately disclosing to Plaintiff and the New Hampshire Subclass Defendant did not follow industry best practices for the collection, use, and storage of SPI.

146. Defendant's conduct, as described herein, constitutes willful and/or knowing violations of the NHCPA.

147. As a direct and proximate result of Defendant's conduct, Plaintiff and the New Hampshire Subclass have been harmed and have suffered damages including, but not limited to: damages arising from attempted identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

148. As a direct and proximate result of Defendant's fraudulent, deceptive, and unfair practices and omissions, Plaintiff and the New Hampshire Subclass' SPI was disclosed to third parties without authorization, causing and will continue to cause Plaintiffs and the New Hampshire Subclass damages. Accordingly, Plaintiffs and the New Hampshire Subclass are entitled to recover damages in accordance with the NHCPA, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against the Defendant and the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' SPI;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

iv. prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database (if, in fact, it does so);

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party

security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the

preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to regularly purge the SPI of the Applicant Subclass;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For pre- and postjudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED: February 27, 2024

Respectfully Submitted,

By: /s/ Robert J. Maselek, Jr.

Robert J. Maselek, Jr.
MCDONOUGH COHEN & MASELEK, LLP
53 State Street, Suite 500
Boston, MA 02109
Direct: 617.742.6520 (Ext. 246)
Fax: 617.742.1393
rmaselek@mcmlawfirm.com

Local Counsel for Plaintiff and the Putative Class

Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

Attorney for Plaintiff and the Putative Class

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Casey Whalen and Luke Millspaugh, Individually and on Behalf of All Others Similarly Situated

(b) County of Residence of First Listed Plaintiff Rockingham, NH
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Robert J. Maselek, Jr.
McDonough Cohen & Maselek LLP
53 State Street, Suite 500, Boston, MA 02109, 617-742-6520

DEFENDANTS

Emmanuel College

County of Residence of First Listed Defendant Suffolk
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Failure to properly secure and safeguard plaintiffs' personal information

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ $5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions):*

JUDGE Judge Kelley DOCKET NUMBER 1:24-cv-10314

DATE 2/27/2024

SIGNATURE OF ATTORNEY OF RECORD /s/ Robert J. Maselek, Jr.

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

1. **Title of case (name of first party on each side only)** Casey Whalen, et al v. Emmanuel College

2. **Category in which the case belongs based upon the numbered nature of suit code listed on the civil cover sheet. (See local rule 40.1(a)(1)).**

☐ **I.** **160, 400, 410, 441, 535, 830*, 835*, 850, 880, 891, 893, R.23, REGARDLESS OF NATURE OF SUIT.**

☐ **II.** **110, 130, 190, 196, 370, 375, 376, 440, 442, 443, 445, 446, 448, 470, 751, 820*, 840*, 895, 896, 899.**

☑ **III.** **120, 140, 150, 151, 152, 153, 195, 210, 220, 230, 240, 245, 290, 310, 315, 320, 330, 340, 345, 350, 355, 360, 362, 365, 367, 368, 371, 380, 385, 422, 423, 430, 450, 460, 462, 463, 465, 480, 485, 490, 510, 530, 540, 550, 555, 560, 625, 690, 710, 720, 740, 790, 791, 861-865, 870, 871, 890, 950.**

***Also complete AO 120 or AO 121. for patent, trademark or copyright cases.**

3. **Title and number, if any, of related cases. (See local rule 40.1(g)). If more than one prior related case has been filed in this district please indicate the title and number of the first filed case in this court.**

Parchinskya v. The Trustees of Emmanuel College 1:24-cv-10314

4. **Has a prior action between the same parties and based on the same claim ever been filed in this court?**

YES ☐ **NO** ☑

5. **Does the complaint in this case question the constitutionality of an act of congress affecting the public interest? (See 28 USC §2403)**

YES ☐ **NO** ☑

If so, is the U.S.A. or an officer, agent or employee of the U.S. a party?

YES ☐ **NO** ☐

6. **Is this case required to be heard and determined by a district court of three judges pursuant to title 28 USC §2284?**

YES ☐ **NO** ☑

7. **Do all of the parties in this action, excluding governmental agencies of the United States and the Commonwealth of Massachusetts ("governmental agencies"), residing in Massachusetts reside in the same division? - (See Local Rule 40.1(d)).**

YES ☑ **NO** ☐

A. **If yes, in which division do all of the non-governmental parties reside?**

Eastern Division ☑ **Central Division** ☐ **Western Division** ☐

B. **If no, in which division do the majority of the plaintiffs or the only parties, excluding governmental agencies, residing in Massachusetts reside?**

Eastern Division ☐ **Central Division** ☐ **Western Division** ☐

8. **If filing a Notice of Removal - are there any motions pending in the state court requiring the attention of this Court? (If yes, submit a separate sheet identifying the motions)**

YES ☐ **NO** ☐

(PLEASE TYPE OR PRINT)

ATTORNEY'S NAME Robert J. Maselek, Jr.

ADDRESS McDonough Cohen & Maselek, LLP, 53 State Street, Suite 500, Boston, MA 02109

TELEPHONE NO. 617-742-6520